Mer om grupper: Eksempler

Def. En avbildning $f: X \to Y$ mellom to mengder kalles

* <u>injektiv</u> dersom det for hver $y \in Y$ finns høyst en $x \in X$ slik at $f(x) = y$.
* <u>surjektiv</u> dersom det for hver $y \in Y$ finns minst en $x \in X$ slik at $f(x) = y$.
* <u>bijektiv</u> dersom det for hver $y \in Y$ finns nøyaktig en $x \in X$ slik at $f(x) = y$.

Altså: bijektiv = injektiv + surjektiv.

Eks: ① $\exp: \mathbb{R} \to \mathbb{R}$ er injektiv, men ikke surjektiv:

Inj.: $e^{x_1} = e^{x_2} \Rightarrow e^{x_1 - x_2} = 1 \Rightarrow x_1 = x_2$

Ikke surj: Fordi $e^x > 0$.

② $\cos: \mathbb{R} \to [-1,1)$ er surjektiv, men ikke injektiv.

Surj: La $y \in [-1,1)$, $x = \arccos(y)$.

Da er $\cos x = y$.

Ikke injektiv: Fordi $\cos(x + 2\pi) = \cos x$ for alle $x \in \mathbb{R}$

Prop: La G være en gruppe og $g \in G$. Da er avbildningen

$$l_g : G \to G, \quad l_g(x) = gx$$

bijektiv.

Bevis: La $y \in G$. Da har likningen

$y = gx$ nøyaktig én løsning x,

nemlig $x = g^{-1}y$. Altså er l_g bijektiv. //

Husk: For $n \geq 1$ er

S_n = gruppa av alle bijeksjoner

$$\{1, \cdots, n\} \to \{1, \cdots, n\},$$

hvor den binære operasjonen er sammensetning av avbildninger.

Merk: Elementene i S_n kalles ofte

permutasjoner.

Notasjon: $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$

betegner elementet $\sigma \in S_4$ gitt ved

$$\sigma(1) = 3, \ \sigma(2) = 1, \ \sigma(3) = 4, \ \sigma(4) = 2.$$

Def: For $\sigma \in S_n$ definerer vi

$$\operatorname{sgn}(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i} = \pm 1.$$

Eks: $n = 3$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\operatorname{sgn}(\sigma) = \frac{(1-3)(2-3)(2-1)}{(2-1)(3-1)(3-2)} = 1.$$

$(i,j) = (1,2) \quad (1,3) \quad (2,3)$

Prop: For $\sigma, \tau \in S_n$ er

$$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau).$$

Altså er $\operatorname{sgn} : S_n \to C_2 = \{\pm 1\}$

en gruppehomomorfi.

Bevis: $\operatorname{sgn}(\sigma\tau) = \prod_{i<j} \frac{\sigma\tau(j) - \sigma\tau(i)}{j - i}$

$$= \prod_{i<j} \frac{\sigma\tau(j) - \sigma\tau(i)}{\tau(j) - \tau(i)} \cdot \prod_{i<j} \frac{\tau(j) - \tau(i)}{j - i}$$

$$= \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau). \quad //$$

Def: En permutasjon $\sigma \in S_n$ kalles en transposisjon dersom det finnes i, j med $i \neq j$ slik at

$$\sigma(i) = j, \quad \sigma(j) = i,$$

$$\sigma(k) = k \text{ for } k \notin \{i, j\}.$$

Eks: $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$ bytter om 2, 4.

Prop: Hvis $\sigma \in S_n$ er en transposisjon, så er $\operatorname{sgn}(\sigma) = -1$.

Bevis: (i) La $\rho \in S_n$ være transposisjonen som bytter om 1 og 2.

$$\frac{\rho(j)-\rho(i)}{j-i} = \begin{cases} \frac{1-2}{2-1} = -1, & i=1,\ j=2 \\ \frac{j-2}{j-1}, & i=1,\ j>2 \\ \frac{j-1}{j-2}, & i=2,\ j>2 \\ \frac{j-i}{j-i} = 1, & i>2 \end{cases}$$

$$\operatorname{sgn}(\rho) = -\prod_{j=3}^{n} \frac{j-2}{j-1}\cdot\frac{j-1}{j-2} = -1.$$

(ii) La σ være transposisjonen som bytter om i og j. Velg en $\tau \in S_n$ med $\tau(i)=1$, $\tau(j)=2$. Da er $\rho = \tau\sigma\tau^{-1}$ som i punkt (i), og

$\sigma = \tau^{-1} \beta \tau$, $\quad sgn(\sigma) = sgn(\tau)^{-1} sgn(\beta) sgn(\tau)$

$= sgn(\beta) = -1.$ //

Prop: Ethvert element i S_n kan skrives som et produkt av transposisjoner.

Eks: $n=4$ $\quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$

$$\underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}}_{\tau_1} \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}}_{\sigma} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$$

$$\underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}}_{\tau_2} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}}_{\tau_3}$$

$\tau_2 \tau_1 \sigma = \tau_3 \quad \Rightarrow \quad \sigma = \tau_1 \tau_2 \tau_3$

$\Rightarrow sgn(\sigma) = (-1)^3 = -1.$

Def: En permutasjon $\sigma \in S_n$ kalles

* <u>jevn</u> dersom $\operatorname{sgn}(\sigma) = 1$,

* <u>odde</u> dersom $\operatorname{sgn}(\sigma) = -1$.

<u>Def</u>: Den <u>alternerende</u> gruppa A_n er definert ved

$A_n :=$ kjernen til $\operatorname{sgn}: S_n \to C_2$

$=$ gruppa av jevne permutasjoner av $\{1, 2, \dots, n\}$.

<u>Prop</u>: $|S_n| = n! = 1 \cdot 2 \cdot 3 \cdots n$.

<u>Bevis</u>: For å definere en $\sigma \in S_n$ kan vi velge verdiene $\sigma(1), \sigma(2), \dots, \sigma(n)$ successivt.

For $\sigma(1)$ har vi n muligheter: $\{1, \dots, n\}$.

For $\sigma(2)$ har vi $n-1$ muligheter: $\{1, \dots, n\} - \{\sigma(1)\}$

For $\sigma(3)$ har vi $n-2$ muligheter

$\vdots$

For $\sigma(n)$ har vi 1 mulighet.

Tilsammen gir det $n \cdot (n-1)(n-2) \cdots 1 = n!$ muligheter. //

<u>Prop</u>: $|A_n| = \frac{n!}{2}$ for $n \geq 2$.

<u>Bevis</u>: Fordi $\operatorname{sgn}: S_n \to C_2$ er en surjektiv gruppehomomorfi, er

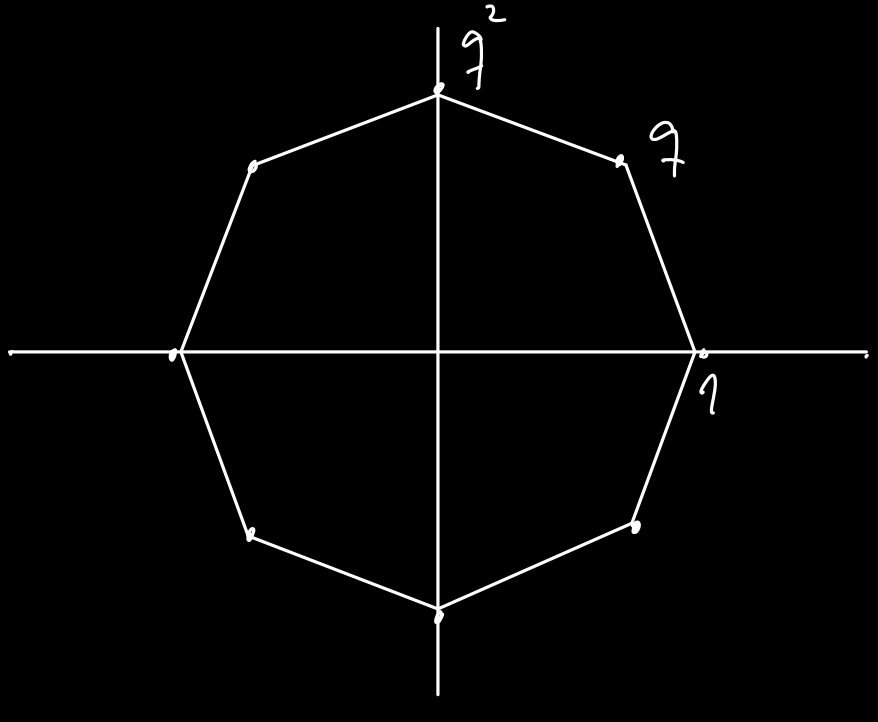
$$|S_n| = |\ker(\operatorname{sgn})| \cdot |C_2|$$

$$= |A_n| \cdot 2$$

$\Rightarrow |A_n| = \frac{1}{2}|S_n| = \frac{n!}{2}$. //

<u>Def</u>: For $n \geq 2$ er diedergruppa D_n definert som symmetrigruppa til et regulært polygon i $\mathbb{R}^2$ med n kanter.

Vi kan velge polygonet i $\mathbb{R}^2 = \mathbb{C}$ med hjørner $\{1, q, q^2, \dots, q^{n-1}\}$, hvor $q = e^{2\pi i/n}$.



$n = 8$

ρ = rotasjonen om origo med vinkel $\frac{2\pi}{n}$

μ = speilingen om x-aksen

Som mengde er

$$D_n = \{Id, \rho, \cdots, \rho^{n-1}, \mu, \mu\rho, \cdots, \mu\rho^{n-1}\}$$

$$\Rightarrow |D_n| = 2n.$$

Som for D_4 finner vi ellers at

$$\mu\rho = \rho^{-1}\mu,$$

og D_n har presentasjonen

$$D_n = \langle \rho, \mu \mid \rho^n = \mu^2 = Id, \ \mu\rho = \rho^{-1}\mu \rangle.$$

7.3 Den ortogonala gruppen $O(3)$

Def: En **symmetri** av en delmängd $F \subset \mathbb{R}^n$ är en isometri $m : \mathbb{R}^n \to \mathbb{R}^n$ sådan att

$$m(F) = F.$$

$\mathrm{Sym}(F)$ = gruppen av alla symmetrier av F.

$\mathrm{Sym}_0(F)$ = gruppen av alla orienteringsbevarande symmetrier av F.

$\subset$ $\mathrm{Sym}(F)$.
undergrupp

Def: En delmängd $F \subset \mathbb{R}^n$ kallas **begränsad** om det finns en konstant $M > 0$ sådan att $\|x\| \leq M$ för alla $x \in F$.



Teorem: Hvis $F \subset \mathbb{R}^n$ er en begrenset mengde, så har $Sym(F)$ et fikspunkt $p \in \mathbb{R}^n$, dvs. $m(p) = p$ for alle $m \in Sym(F)$.

Bevis: Utelatt.

Husk Den Euklidiske gruppa $E(n)$ består av alle isometrier $\mathbb{R}^n \to \mathbb{R}^n$.

Teorem Enhver endelig undergruppe G av $E(n)$ har et fikspunkt.

Bevis: Sett $n = |G|$ og velg $p \in \mathbb{R}^n$.

Vi vil vise at

$$q = \frac{1}{n} \sum_{g \in G} g(p)$$

er et fikspunkt for G. La $h \in G$.

Vi kan skrive

$$h(x) = Ax + v, \qquad (x \in \mathbb{R}^n)$$

hvor $A \in O(n)$ og $v \in \mathbb{R}^n$. Da er

$$h(q) = \frac{1}{n} \sum_{g \in G} Ag(p) + v$$

$$= \frac{1}{n} \sum_{g \in G} (Ag(p) + v)$$

$$= \frac{1}{n} \sum_{g \in G} (hg)(p)$$

$$= \frac{1}{n} \sum_{g \in G} g(p)$$

$$= q. \quad //$$

<u>Anvendelse</u>: Anta $q \in \mathbb{R}^n$ er et fikspunkt for $Sym(F)$, $F \subset \mathbb{R}^n$, og sett

$$F' = F - q = \{x - q \mid x \in F\}.$$

Da er $\mathrm{Sym}(F') \cong \mathrm{Sym}(F)$, og 0 er et fikspunkt for F'. Altså består $\mathrm{Sym}(F')$ kun av punktsymmetrier og kan derfor identifiseres med en undergruppe av $O(n)$.

Husk: En punktsymmetri har formen

$$m(x) = Ax, \quad \text{hvor } A \in O(n).$$